EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ambassadors.es/	Checks	9 pruebas
Dominio	ambassadors.es	Hallazgos	48 totales
Fecha	25 de agosto de 2026 a las 19:38	Problemas	20 detectados

D

41/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio ambassadors.es ha arrojado una puntuación de 41/100, lo que equivale a una nota de D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales únicamente 4 fueron superados satisfactoriamente, mientras que 5 presentaron fallos críticos. Los resultados indican una carencia total de cabeceras de seguridad y una exposición peligrosa de puertos de infraestructura interna. En su estado actual, el sitio se considera vulnerable y presenta riesgos significativos para la integridad de los datos y la privacidad de los usuarios.

Resumen de Riesgos

1	7	10	2	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-11-02T17:27:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-04T17:27:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 301 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.1

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ambassadors.es/wp-content/uploads/elementor/css/b...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ambassadors.es/wp-content/uploads/elementor/css/l...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ambassadors.es/wp-content/uploads/elementor/css/b...
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (68 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://www.dekhome.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy

INFO **Puerto 27017 (MongoDB)**

Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL): La base de datos está abierta a conexiones externas, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Content-Security-Policy: Esta cabecera está ausente, dejando al sitio vulnerable a ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta configuración permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga a realizar conexiones seguras mediante HTTPS.
[HIGH] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico inseguro al protocolo cifrado, exponiendo la información en tránsito.
[HIGH] WordPress versión expuesta: Se detectan versiones como la 7.1 expuestas públicamente, lo que permite a atacantes identificar vulnerabilidades conocidas (CVEs).
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que envía credenciales y datos sin cifrar por la red.
[MEDIUM] Contenido Mixto: Se han detectado 4 recursos cargados mediante HTTP dentro de la página protegida por SSL, rompiendo la cadena de seguridad.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de sniffing.
[MEDIUM] Referrer-Policy: No existe control sobre la información de procedencia que se envía a otros dominios al hacer clic en enlaces.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a componentes sensibles como la cámara o el micrófono.
[MEDIUM] Archivos y rutas expuestas: El archivo /readme.html y la ruta de acceso /wp-login.php son accesibles, revelando información técnica del CMS.
[MEDIUM] Puerto 22 (SSH): El puerto de administración remota está abierto, incrementando la superficie de ataque del servidor.
[LOW] Server header: El servidor revela el uso de Apache, proporcionando información útil para que un atacante personalice sus herramientas de explotación.
[LOW] Meta generator: La etiqueta meta expone la versión exacta de WordPress en el código fuente del sitio.